

What is claimed is:

CLAIMS:

- 1 1. In an information handling system for identifying network resources
2 comprising packets of data received from a network, a method comprising:
3 receiving a network resource comprising one or more packets, each packet
4 comprising a header and data portion;
5 scanning the bytes of the one or more packets to determine the application-
6 level protocol, and thus the application, the sender of the bytes is using.
7 parsing the bytes of the one or more packets according to the specific
8 application-level protocol to extract identifying information relating to a specific
9 resource requested;
10 comparing the extracted information to a list of identifying information stored
11 in a real-time database; and
12 providing a message indicating that the extracted information matches at least
13 one entry in the real-time database when the comparison is positive.
- 1 2. The method of claim 1, wherein the receiving step comprises receiving a
2 plurality of packets according to the Transmission Control Protocol.
- 1 3. The method of claim 1, wherein the receiving step comprises receiving a
2 plurality of packets according to the User Datagram Protocol.

- 1 4. The method of claim 1 wherein the one or more packets use the hypertext
2 transfer protocol, the scanning step comprises extracting a destination domain name or
3 IP address from a hypertext transfer protocol packet stream and the comparing step
4 comprises comparing the address extracted with addresses stored in the database.
- 1 5. The method of claim 1 wherein the one or more packets follow the hypertext
2 transfer protocol and the scanning step further comprises extracting the port, path, and
3 name of the web resource from a hypertext transfer protocol packet stream.
- 1 6. The method of claim 1 wherein, the scanning step comprises extracting a hash
2 code from a received peer to peer protocol packet stream.
- 1 7. The method of claim 1 wherein, the scanning step comprises extracting
2 additional information comprising port, identity key, and filename from a peer to peer
3 protocol packet stream.
- 1 8. The method of claim 1 wherein, the scanning step comprises extracting a user
2 agent name, additional HTTP extension headers, or other information needed to
3 identify a specific program from a peer to peer protocol packet stream.
- 1 9. The method of claim 1 wherein, the scanning step comprises extracting a
2 filename and path received from a file transfer protocol packet stream.
- 1 10. The method of claim 1 wherein the scanning step further comprises detecting a
2 transmission control protocol connection to an external simple mail transfer protocol
3 server, and limiting access to the external simple mail transfer protocol server.

- 1 11. The method of claim 1 further comprising logging all instant message
2 communication.
- 1 12. The method of claim 1 further comprising providing a message announcing a
2 match upon identifying the match.
- 1 13. The method of claim 1 wherein, the comparing step, upon identifying a match,
2 further comprises blocking the user from accessing the resource corresponding to the
3 matching identifying information.
- 1 14. The method of claim 1 wherein the identifying information corresponds to
2 illegal copies of files.
- 1 15. The method of claim 1 wherein the identifying information corresponds to
2 prohibited resources.
- 1 16. The method of claim 1 wherein the scanning step comprises extracting an IP
2 address from at least one packet and the comparing step comprises comparing the IP
3 address with a set of IP addresses stored in the database.
- 1 17. The method of claim 1 wherein the identifying information comprises a hash
2 code.
- 1 18. The method of claim 1 wherein the identifying information corresponds to
2 suspicious files and wherein a client requesting a file whose identifying information
3 matches an identifying information stored in the database is presented a warning.

1 19. The method of claim 1 wherein, the comparing step upon identifying a match
2 further comprises limiting access by clients to external simple mail transfer protocol
3 servers.

1 20. The method of claim 1 further comprising using identifying information found
2 by a central server farm comprising specialized search engines and a human staff to
3 populate the database.

1 20. The method of claim 13 wherein the blocking step is accomplished by ending
2 client/server communication for a request that contains the matching identifying
3 information.

1 21. The method of claim 13 wherein the blocking step is accomplished by ending
2 client/server communication for a response that contains the matching identifying
3 information.

1 22. The method of claim 1 wherein the receiving step comprises receiving a
2 plurality of packets according to the Simple Mail Transfer Protocol.

1 23. The method of claim 1, wherein the scanning step further evaluates additional
2 headers and the data portion of the hypertext transfer protocol, such as web forms on
3 an html page, based on the address.

1 24. A system comprising:
2 a network interface for receiving data packets from a network;

3 a processor for extracting identifying information from the data packets and for
4 comparing the extracted identifying information with the identified information stored
5 in a database; and
6 an output for providing a message stating when a match has been found.

1 25. The system of claim 24 further comprising a memory for storing the identified
2 information to be compared with the information extracted from the received packets.

1 26. A local area network comprising a network gateway device comprising: a
2 network interface for receiving data packets; a processor for extracting identifying
3 information and for comparing the extracted identifying information with the
4 identifying information stored in a database; and an output for providing a message
5 stating that a match has been found when the comparison is positive.

1 27. The local area network of claim 26 further comprising the database.

1 28. The local area network of claim 26 further comprising a router disposed
2 between the network gateway device and a firewall connecting the local area network
3 to a wide area network.

1 29. The local area network of claim 26 further comprising a load balancer disposed
2 between the router and a firewall.

1 30. The local area network of claim 26 further comprising a network gateway
2 device disposed between a router and a load balancer.

1 31. The local area network of claim 26 further comprising a load balancer disposed

2 between the network gateway device and a firewall connecting the local area network
3 to a wide area network.

1 32. The local area network of claim 26 further comprising a router containing the
2 network gateway device.

1 33. The local area network of claim 26 further comprising a firewall disposed
2 between the router containing the network gateway device and the wide area
3 network.

1 34. The local area network of claim 26 further comprising a firewall containing the
2 network gateway device.

1 35. The local area network of claim 26 further comprising the firewall containing
2 the network gateway device disposed between a router and the wide area network.